PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: Thomas Schneck
Schneck & Schneck
P.O. Box 2-E
San Jose, California 95109-0005

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	19 OCT 2007
Applicant's or agent's file reference: ATM-329	FOR FURTHER ACTION: See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US 06/13795	12 April 2006 (12.04.2006)	12 May 2005 (12.05.2005)

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - H04L 9/00 (2007.01)
USPC - 713/174

Applicant: Atmel Corporation

1. This opinion contains indications relating to the following items:

- [x] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [x] Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	12 June 2007 (12.06.2007)	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 06/13795

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed

☐ filed together with the international application in electronic form

☐ furnished subsequently to this Authority for the purposes of search

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 06/13795

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	None	YES
	Claims	1-11	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-11	NO
Industrial applicability (IA)	Claims	1-11	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-11 lack novelty under PCT Article 33(2) as being anticipated by US 2002/0055962 A1 (Schroeppel). Schroeppel teaches a method and apparatus for speeding up cryptographic calculations.

As to claim 1, Schroeppel teaches a cryptographically secure, computer hardware- implemented modular polynomial reduction method in the binary finite field GF (2n), comprising: precomputing and storing in memory a polynomial constant u (x) representing a bit-scaled reciprocal of a polynomial modulus m(x) (para[0080]); estimating an approximate polynomial quotient q for a polynomial p (x) to be reduced modulo m (x) , wherein said estimating is executed upon p (x) in a computation unit by a polynomial multiplication over GF (2n) by said constant u (x) and by bits shifts (para[0092]-[0093]); generating in a random number generator a random polynomial error value E (x) and applying said polynomial error value to said approximate polynomial quotient to obtain a randomized polynomial quotient q' (x) = q(x) + E(x) (para[0059]); and calculating a polynomial remainder r' (x) = p (x) + q' (x) m(x) in said computation unit, said remainder r' (x) being of high degree than said modulus m(x) but congruent to p (x) modulo m(x) and where the degree of p (x) is less than or equal to 2k+l (para [0111]-[0112]).

As to claim 2, Schroeppel teaches the method of claim 1 wherein precomputing said polynomial constant u (x) is performed according to the equation u (x) = x2k+w/m(x) (para[0114]).

As to claim 3, Schroeppel teaches the method of claim 2 wherein estimating the quotient q (x) is performed by the computation unit according to the equation q(x) = ((p (x) /x1**1) -u(x))/xk+2 (para[0092]-[0093]).

As to claim 4, Schroeppel teaches the method of claim 1 wherein said bit shifts are word-size shifts, the polynomial constant is precomputed as u (x) = x2k+w/m(x) and the quotient is estimated as q(x) = ((p (x) /xk**w) -u(x)) /xk+2w, where w is the word size in bits, and where the degree of p (x) is less than or equal to 2k + w (para[0091]-[0092]).

As to claim 5, Schroeppel teaches the method of claim 4 wherein the random number generator has a specified error limit of one-half word, whereby 0 < deg(E(x)) < w/2 (para[0059]).

As to claim 6, Schroeppel teaches the method of claim 1 wherein the modular reduction of p (x) is part of a computer hardware-implemented cryptography program (para[0094]-[0096]).

As to claim 7, Schroeppel teaches computational hardware for executing a cryptographically secure polynomial modular reduction method over a binary finite field GF (2) , the hardware comprising: a computation unit adapted to perform word-wide finite-field multiply and accumulate steps on polynomial operands retrieved from a memory and polynomial coefficient intermediate results from a set of working registers (para[0093] and [0118]-[0121]); a random number generator for generating a random polynomial error value E (x) (para[0059]); an operations sequencer comprising logic circuitry for controlling the computation unit and random number generator in accord with program instructions so as to carry out a polynomial modular reduction of a number p (x) with respect to a modulus m(x) over a binary finite field GF (2n) that involves at least an estimation of a polynomial quotient q (x) from a pre-stored polynomial constant u (x) representing a bit-scaled reciprocal of the modulus, a randomization of said the approximate polynomial quotient with said random polynomial error value E (x) to obtain a randomized polynomial quotient q' (x) = q (x) + E (x) , and a calculation of a polynomial remainder value r' (x) = p (x) + q' (x) m (x) (para[0059], [0077], [0096]).

As to claim 8, Schroeppel teaches the computation hardware of claim 7 further comprising operation parameter registers accessible by said operations sequencer, said registers containing any one or more of (a) pointers for locating word-size coefficients of polynomial operands within said memory or working registers (para[0093]), (b) information about word lengths of polynomial operands (para[0111]), and (c) destination address information for intermediate results of operation steps (para[0018]).

As to claim 9, Schroeppel teaches the computation hardware of claim 7 wherein the pre- stored polynomial constant u (x) in said memory is obtained from a precomputation according to the equation u (x) = x2k+w/m (x) , with w being the word size of the computation unit in bits (para[0112]-[0114]).

- Please See Continuation Sheet -

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V.2. Citations and explanations:

As to claim 10, Schroeppel teaches the computation hardware of claim 9 wherein the estimation of said approximate polynomial quotient q performed by said computation unit under control of said operations sequencer carrying out program instructions is done according to the equation q' (X) = ((P(X) -xk°w) -u(x))/xk+2w (para[0080], [0093]).

As to claim 11, Schroeppel teaches the computation hardware of claim 10 wherein the random number generator has a specified error limit of one-half word, whereby 0 < deg (E(x) < w/2 (para[0059]).

Claims 1-11 have industrial applicability as defined by PCT Article 33(4) because the subject matter can be made or used in industry.